Los mantenedores del proyecto OpenSSL lanzaron parches para abordar una vulnerabilidad de alta gravedad en la biblioteca criptográfica que podría conducir a la ejecución remota de código en algunos escenarios.

El problema, que se rastrea con el identificador CVE-2022-2274, se describió como un caso de corrupción de la memoria en montón con la operación de clave privada RSA, que se introdujo en la versión 3.0.4 de OpenSSL lanzada el 21 de junio de 2022.

Lanzado por primera vez en 1998, OpenSSL es una biblioteca criptográfica de propósito general que ofrece una implementación de código abierto de los protocolos Secure Sockets Layer (SSL) y Transport Layer Security (TLS), lo que permite a los usuarios generar claves privadas, crear solicitudes de firma de certificados (CSR) e instalar certificados SSL/TLS.

> *«Los servidores SSL/TLS u otros servidores que utilizan claves privadas RSA de 2048 bits que se ejecutan en las máquinas que admiten instrucciones AVX512IFMA de la arquitectura x86_64 se ven afectados por este problema»,* dice el aviso.

Llamándolo un *«error grave en la implementación de RSA»*, los mantenedores afirmaron que la vulnerabilidad podría conducir a la corrupción de la memoria durante el cálculo que un atacante podría utilizar como arma para desencadenar la ejecución remota del código en la máquina que realiza el cálculo.

Xi Ruoyao, estudiante de doctorado de la Universidad de Xidia, es a quien se le atribuye haber informado la vulnerabilidad a OpenSSL el 22 de junio de 2022. Se recomienda a los usuarios de la biblioteca que actualicen a OpenSSL versión 3.0.5 para mitigar cualquier amenaza potencial.